FAA Safety Management System (SMS)

2004 Risk Analysis Workshop
August 17, 2004

Roberta Leftwich, Director of Safety Risk Management

Introduction

Safety …. Our highest priority

"Air Traffic Organization is the service arm of the FAA and that the most important characteristic of our service is safety. Essentially, we define what we provide as safety services."

(Russ Chew, 1/9/04)

"…safety is our service…"

(Russ Chew, 1/26/04)

Safety and the SMS

- Safety:
  - Freedom from unacceptable risk
- FAA's SMS:
  - Focuses on NAS safety (safety in the provision of air traffic control and navigation services); not occupational safety (OSHA)
  - Required by:
    - ATO Customers/Owners
    - Air Traffic Safety Oversight Service (AOV)
    - International Civil Aviation Organization (ICAO)
  - Included in *FAA Flight Plan 2004–2008*
  - Will hold FAA accountable for the same level of safety discipline it requires of the aviation industry

Owner/Customer Questions

- ATO owners and customers want to know:
  - On a regular basis:
    - Is the system safe?
    - How do you know?
  - When something bad happens:
    - Could it have been avoided?
    - Did you do all that you could?
    - Why should I be confident it won’t happen again?

Safety Oversight Questions

- Oversight will ask ATO to:
  - Provide safety metrics and the steps being taken to improve them (safety promotion)
  - Define safety critical systems, procedures, and processes
  - Define the number of safety significant changes made last month? Year?
  - Show the process used to demonstrate that safety was assured
  - Provide documentation on major safety critical changes

The ATO … when SMS is fully implemented … will be able to provide these answers

FAA SMS Development

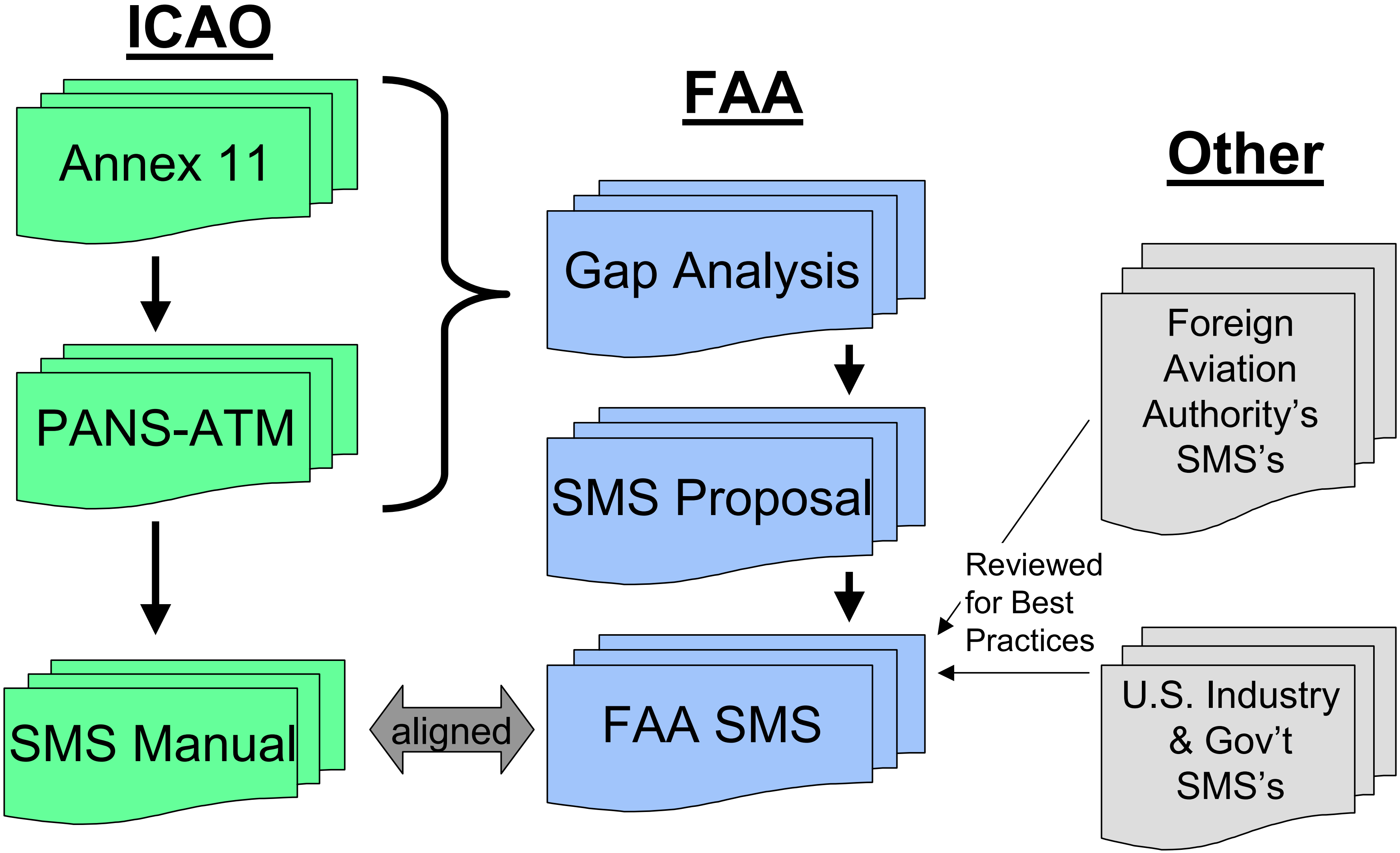
Drivers for SMS Implementation

- In 2000, FAA began studying independent safety oversight and safety management
  - Study showed safety management systems (SMS) are an internationally proven model for efficiently and effectively managing safety
- In 2001, International Civil Aviation Organization (ICAO) amended Annex 11 requiring key safety management elements for air traffic control and navigation service provision
- In 2003, objective under the safety goal in the *FAA Flight Plan 2004-2008* requires implementation of an SMS

Existing Baseline for SMS

- Prior to SMS development, the FAA complied with the majority of ICAO SMS requirements
- SMS integrates with existing FAA processes
  - Processes, procedures, and systems exist that ensure U.S. National Airspace System (NAS) safety, including:
    - System/equipment acquisition management
    - Air traffic control (ATC) unit and equipment quality/safety assurance
    - Operational training and certification programs
    - Accident/incident investigation
  - FAA has published safety goals that are met through internal and external initiatives
  - Detailed operational data is collected and analyzed to improve system safety

Aligning and Leveraging


ICAO
Annex 11
PANS-ATM
SMS Manual
aligned
FAA
Gap Analysis
SMS Proposal
FAA SMS
Other
Foreign Aviation Authority's SMS's
Reviewed for Best Practices
U.S. Industry & Gov't SMS's

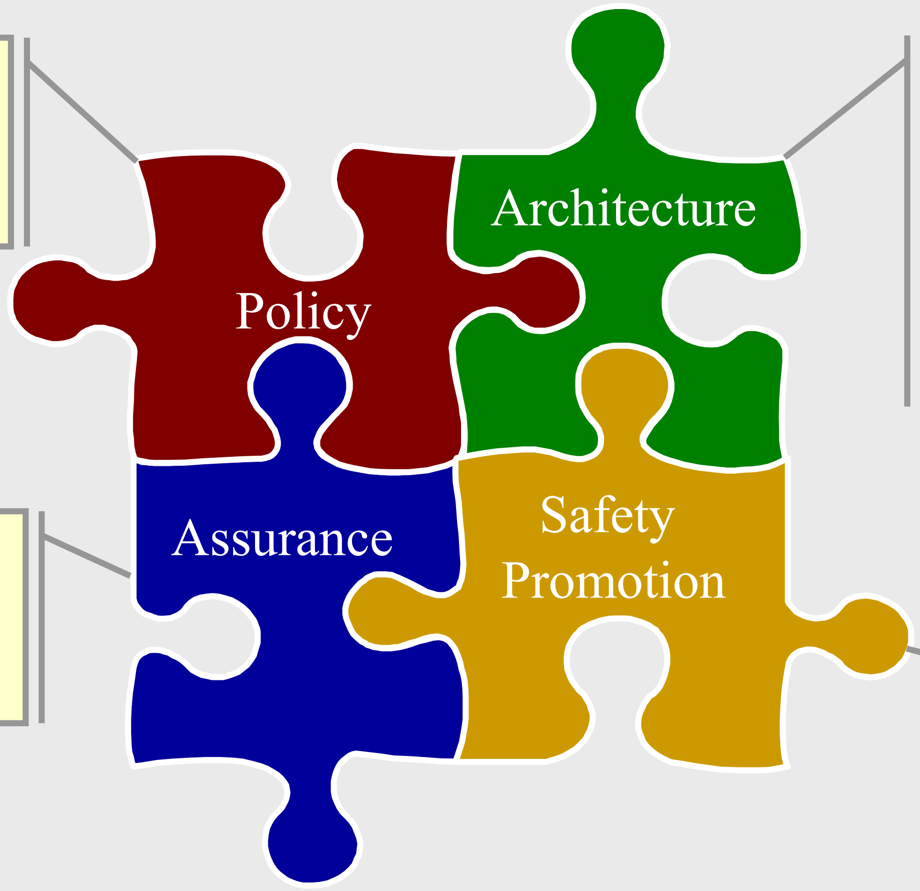
Overview of SMS

SMS Overview

- Goal of SMS implementation is to enhance the safety of the provision of air traffic services:
  - Provides common framework for identifying, assessing, mitigating, and tracking safety risk of National Airspace System (NAS) changes
  - Includes safety assurance (i.e. audits, evaluations, and data analyses)
  - Promotes and strengthens safety culture within FAA through training, dissemination of lessons learned, and sharing of safety data
- FAA SMS as documented in FAA SMS Manual meets/exceeds ICAO requirements

FAA Safety Management System

- SMS Requirements
- SMS Responsibilities & Accountabilities
- Safety Oversight



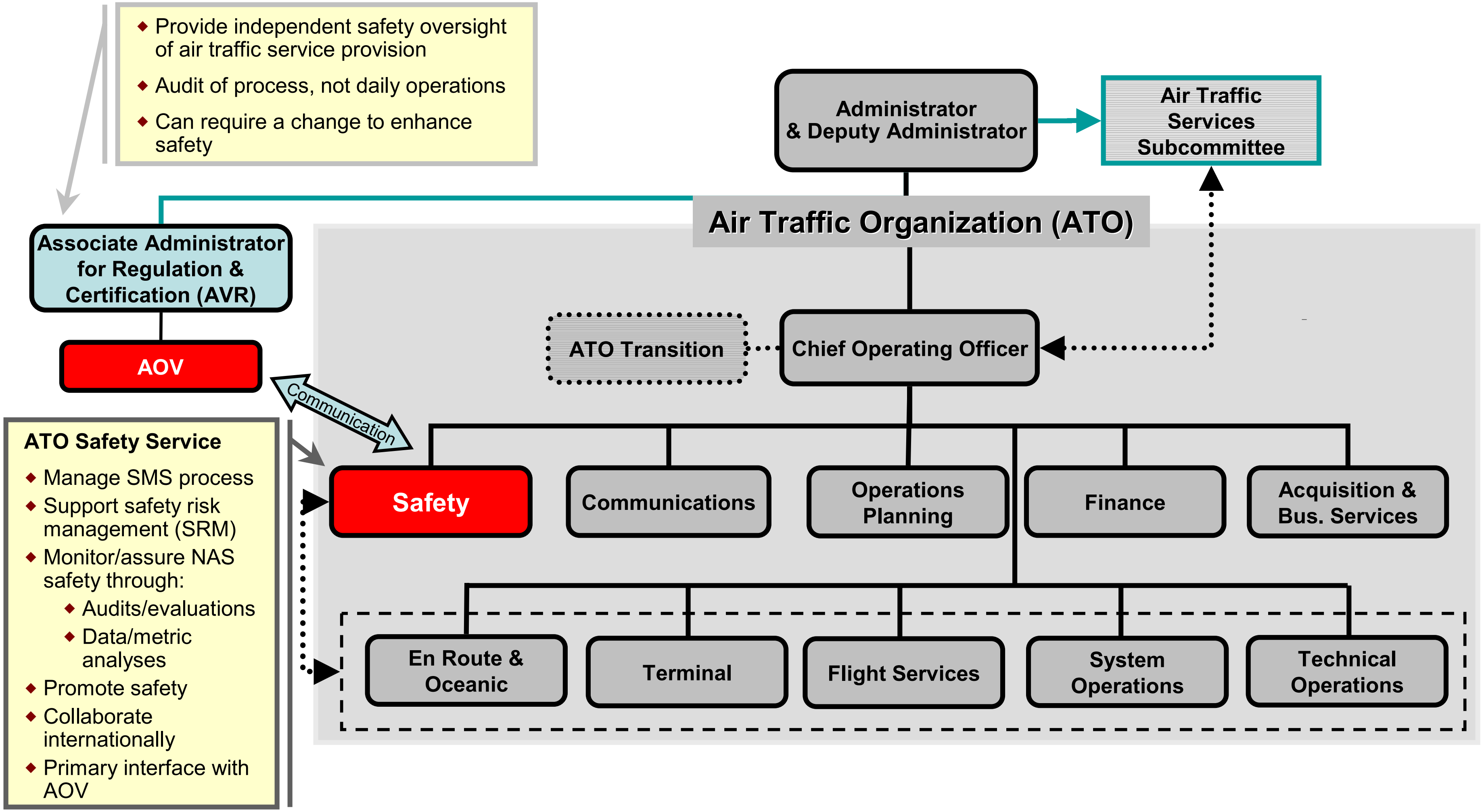
- Safety Risk Management (SRM) - e.g. changes are safe
  - SRM Filter (what changes require SRM?)
  - SRM Guidance
  - SRM Documentation (and who approves)

- Safety Assurance and Evaluations
- Safety Data Tracking and Analysis

- Recommending Actions based on Safety Metrics
- SMS Training
- Safety Organization
  - Safety Culture
  - Safety Lessons Learned

FAA Safety Organizations

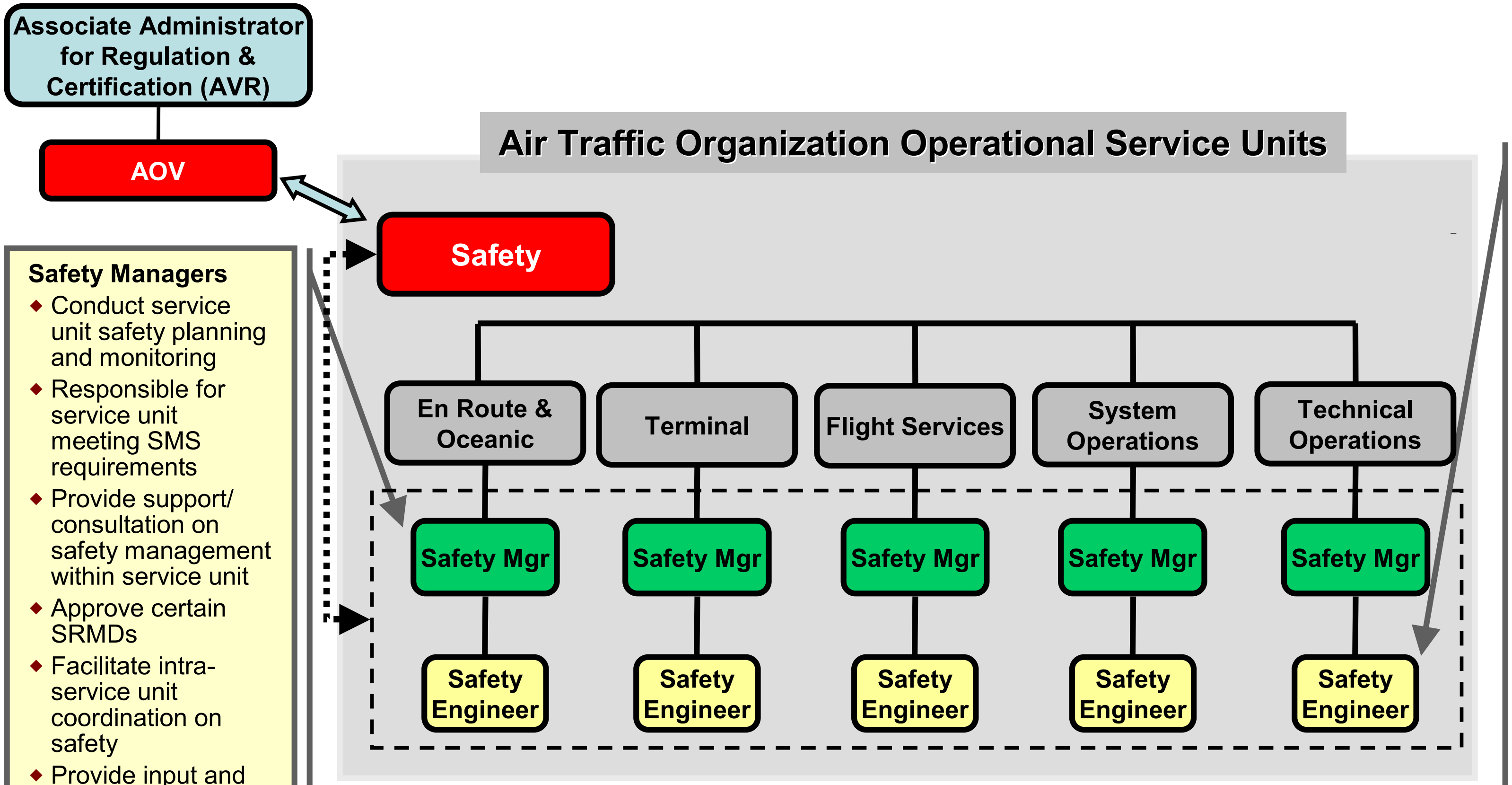
- Provide independent safety oversight of air traffic service provision
- Audit of process, not daily operations
- Can require a change to enhance safety


Administrator & Deputy Administrator
Air Traffic Services Subcommittee
Air Traffic Organization (ATO)
Associate Administrator for Regulation & Certification (AVR)
AOV
ATO Transition
Chief Operating Officer
Communication
Safety
Communications
Operations Planning
Finance
Acquisition & Bus. Services
En Route & Oceanic
Terminal
Flight Services
System Operations
Technical Operations

ATO Safety Service

- Manage SMS process
- Support safety risk management (SRM)
- Monitor/assure NAS safety through:
  - Audits/evaluations
  - Data/metric analyses
- Promote safety
- Collaborate internationally
- Primary interface with AOV

Safety Managers and Safety Engineers in Service Units



Associate Administrator for Regulation & Certification (AVR)

AOV

Air Traffic Organization Operational Service Units

Safety

En Route & Oceanic

Terminal

Flight Services

System Operations

Technical Operations

Safety Mgr

Safety Mgr

Safety Mgr

Safety Mgr

Safety Mgr

Safety Engineer

Safety Engineer

Safety Engineer

Safety Engineer

Safety Engineer

Safety Managers

- Conduct service unit safety planning and monitoring
- Responsible for service unit meeting SMS requirements
- Provide support/ consultation on safety management within service unit
- Approve certain SRMDs
- Facilitate intra-service unit coordination on safety
- Provide input and advice on safety to VP

Safety Engineers

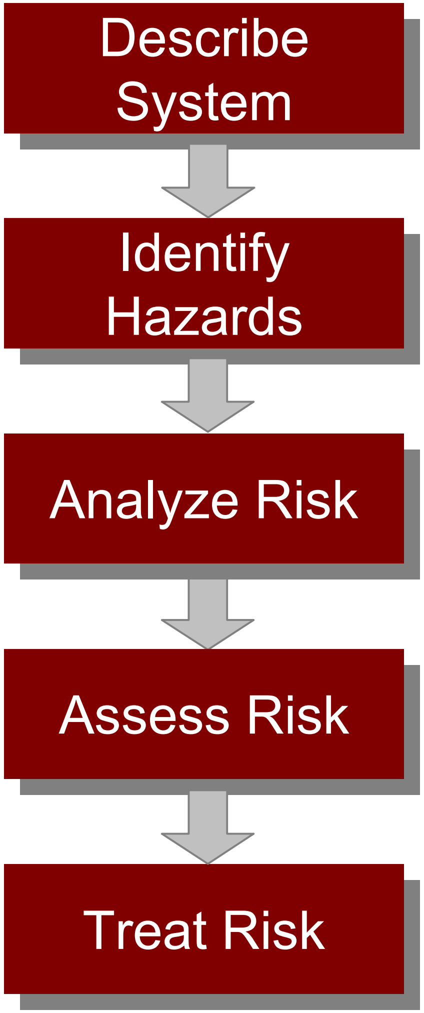
- Support, advise, and assist programs and analysis teams in conducting SRM
- Facilitate SRM decision process and resulting documentation
- Provide recommendations to Safety Manager on SRMD approval
- Provide input to service unit VP, managers, and directors on risk acceptance
- Provide input and advice on safety to VP and Safety Manager

Safety Risk Management (SRM)

Safety Risk Management (SRM)

- SRM is a component of the SMS
- Primary focus of SMS implementation
- Formalized proactive approach to system safety
  - Safety related changes are documented
  - Risk is assessed and analyzed
  - Unacceptable risk is mitigated
  - Hazards are identified and tracked to resolution
  - Effectiveness of risk mitigation strategies are assessed
  - Performance of change is monitored throughout lifecycle

SRM Process



Describe System

- Define scope and objectives
- Define stakeholders
- Identify criteria and plan for risk management effort
- Describe system (use, environment, and intended function, including planned future configuration)

Identify Hazards

- Identify hazards (what can go wrong?) that exist in the context
- Use structured approach
- Be comprehensive (and do not dismiss hazards prematurely)
- Lessons learned and experience supplemented by checklists

Analyze Risk

For each hazard:

- Identify existing mitigations/controls
- Determine risk (severity and likelihood) of outcome
  - Qualitative or quantitative

Assess Risk

- Rank hazards according to the severity and likelihood of their risk
- Select hazards for detailed risk treatment (based on risk)

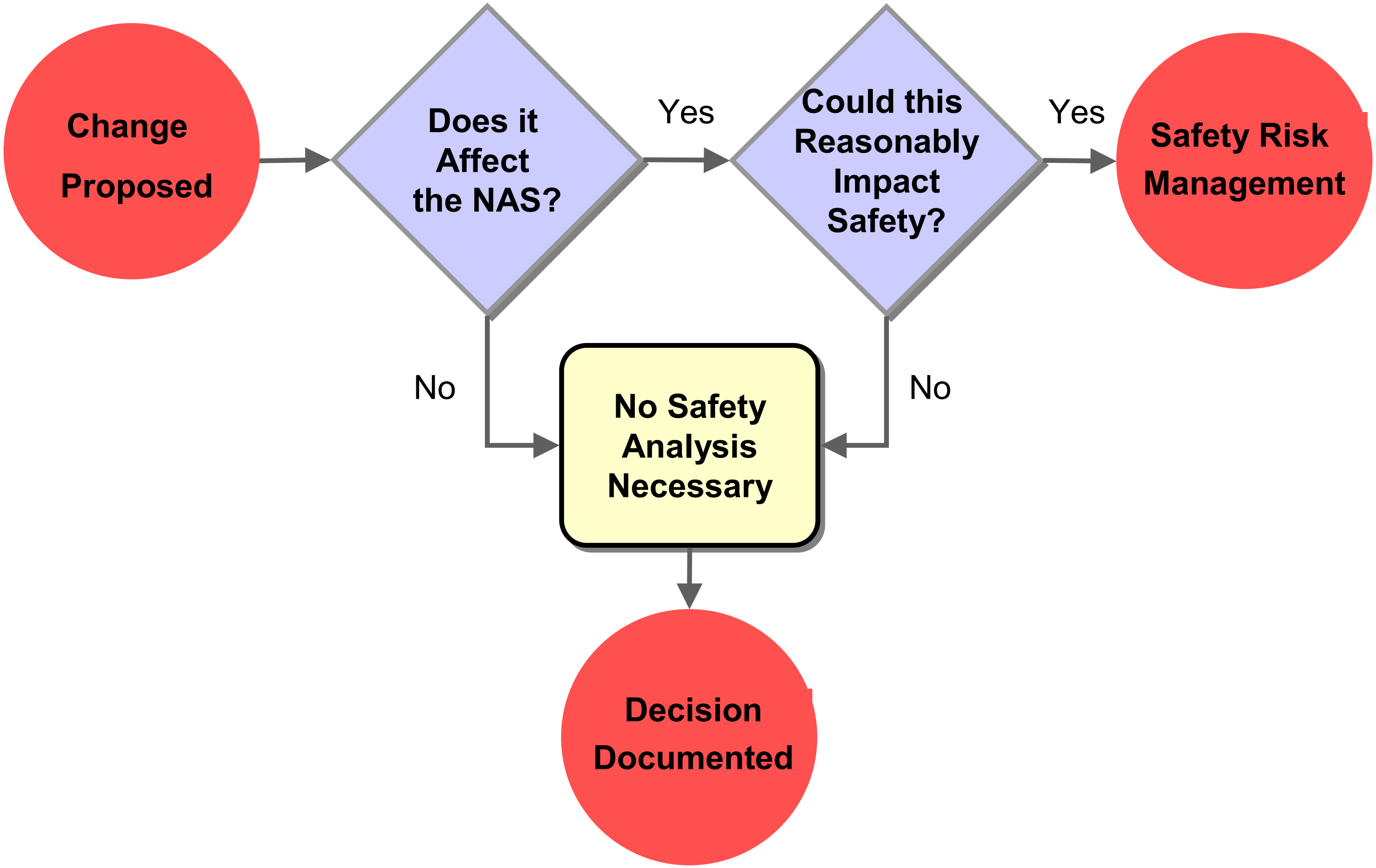
Treat Risk

- Identify feasible mitigation options
- Select best balanced response
- Develop risk treatment plans
- Verify and implement
- Monitor

When is SRM Required?

- Required for all safety significant changes to system or procedures used in the provision of air traffic services, including the following types of changes, at a minimum:
  - Airspace changes
  - Air traffic services procedures and standards
  - Airport procedures and standards
  - New equipment, systems, or facilities
  - Modifications to critical equipment, systems, or facilities

SRM Decision Process



Documenting the Decision

- If SRM is not required:
  - Written statement is required
    - Includes decision and supporting logic
    - Signed by manager
    - Kept on file for lifecycle of system or change
- If SRM is required
  - Follow SRM processes
  - Develop a safety case or “Safety Risk Management Document (SRMD)” matching type and complexity of change that answers:
    - What is the change?
    - How has the safety risk of the change been assessed?
    - What risk has been identified?
    - How will the risks be mitigated and monitored?

Understanding Safety Risk

Severity Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	🟩	🟨	🟥	🟥	🟥
Probable B	🟩	🟨	🟥	🟥	🟥
Remote C	🟩	🟩	🟨	🟥	🟥
Extremely Remote D	🟩	🟩	🟩	🟨	🟥
Extremely Improbable E	🟩	🟩	🟩	🟩	🟨🟥 *

🟥	High Risk
🟨	Medium Risk
🟩	Low Risk

* Unacceptable with Single Point and Common Cause Failures

- High Risk: Unacceptable Risk
  - Cannot be implemented unless hazards are mitigated
  - Tracking and management required
- Medium Risk: Acceptable Risk
  - Acceptable
  - Proposal may be implemented but tracking and management are required
- Low Risk: Target
  - Acceptable
  - Hazards must be documented

What is Severity?

- Severity is determined by the worst credible potential outcome
  - Determined prior to assessing the risk of a hazard occurring
  - Do not consider likelihood when determining severity
  - While less severe effects may be considered analytically, the most severe credible effect must always be considered

Severity

Effect On: ⬇	Hazard Severity Classification				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
General		•Does not significantly reduce system safety (see below):	•Reduces capability to the extent that there would be a (see below):	• Reduces capability to the extent that there would be a (see below):	•Total loss of systems control
Air Traffic Control	• Slight increase in ATC workload	• Slight reduction in ATC capability or significant increase in ATC workload	• Significant reduction in separation or significant reduction in ATC capability	• Total loss of ATC capability, reduction in separation defined by high severity ops error	• Collision with other aircraft, obstacles, or terrain
Flying Public	• No effect on flight crew • No effect on safety • Inconven-ience	• Slight increase in workload • Slight reduction in safety margin • Minor illness, environmental or system damage • Some physical discomfort to occupants	• Significant increase in flight crew workload • Significant reduction in safety margin • Major illness, injury, environmental or system damage • Physical distress on occupants	• Large reduction in safety margin • Serious or fatal injury to small number • Physical distress/excessive workload on flight crew	• Outcome would result in hull loss, multiple fatalities, or fatal injury

What is Likelihood?

- An expression of how often an event is expected to occur
- Severity must be considered when determining likelihood
  - How often resulting harm can be expected to occur at worst credible severity
- Definitions are tailored to domain and service
  - NAS Systems
  - Flight Procedures
  - ATC Operations

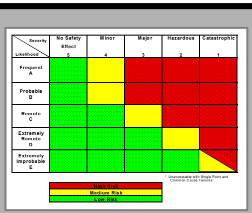
Likelihood Definitions

	NAS Systems			Flight Procedures	ATC Operational	
	Quantitative	Qualitative				
		Individual Item/System	ATC Service/ NAS Level System		Per Facility	NAS-wide
Frequent	Probability of occurrence per operation/ operational hour is equal to or greater than 1x10^{-3}	Expected to occur about once every 3 months for an item	Continuously experienced in the system	Probability of occurrence per operation/ operational hour is equal to or greater than 1x10^{-5}	Expected to occur more than once per week	Expected to occur more than every 1-2 days
Probable	Probability of occurrence per operation/ operational hour is less than 1x10^{-3}, but equal to or greater than 1x10^{-5}	Expected to occur about once per year for an item	Expected to occur frequently in the system		Expected to occur about once every month	Expected to occur about several times per month
Remote	Probability of occurrence per operation/ operational hour is less than or equal to 1x10^{-5} but equal to or greater than 1x10^{-7}	Expected to occur several times in life cycle of an item	Expected to occur numerous times in system life cycle	Probability of occurrence per operation/ operational hour is less than or equal to 1x10^{-5} but equal to or greater than 1x10^{-7}	Expected to occur about once every year	Expected to occur about once every few months
Extremely Remote	Probability of occurrence per operation/ operational hour is less than or equal to 1x10^{-7} but equal to or greater than 1x10^{-9}	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system life cycle	Probability of occurrence per operation/ operational hour is less than or equal to 1x10^{-7} but equal to or greater than 1x10^{-9}	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years
Extremely Improbable	Probability of occurrence per operation/ operational hour is less than 1x10^{-9}	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	Probability of occurrence per operation/ operational hour is less than 1x10^{-9}	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years

Risk Acceptance vs. SRMD Approval

- Accepting the safety risk is a certification by the appropriate management official that he/she understands the safety risk associated with the change and he/she accepts that safety risk into the NAS
- Approving the SRMD (Safety Risk Management Document or safety case) means that the approving party agrees that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate

Risk Acceptance

	High Initial Risk*	Medium or Low Initial Risk
Safety Risk and/or Controls:	Risk Accepted by:	Risk Accepted Within:
Stay Within a Service Unit	Service Unit VP	Service Unit
Span Service Units	Each Affected Service Unit VP	Each Affected Service Unit
Affect LOBs Outside the ATO (e.g., ARP and/or AVR)	Each Affected Service Unit VP and Each Associate Administrator	Each Affected Service Unit and LOB

* Please note that high initial risk must be mitigated to medium or low before acceptance

Severity / Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	🟩	🟨	🟥	🟥	🟥
Probable B	🟩	🟨	🟥	🟥	🟥
Remote C	🟩	🟩	🟨	🟥	🟥
Extremely Remote D	🟩	🟩	🟩	🟨	🟥
Extremely Improbable E	🟩	🟩	🟩	🟩	🟨 / 🟥 *

* Unacceptable with Single Point and Common Cause Failures

🟥 High Risk

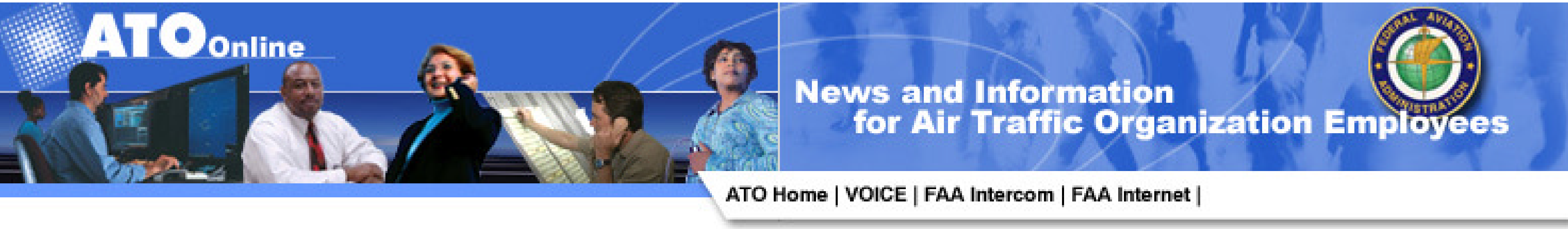
🟨 Medium Risk

🟩 Low Risk

Approvals in SRM

By AOV	SRMD Approved by ATO Safety Service Unit *	SRMD Approved at the Service Director/Manager Level *
•ATO Safety Management System (SMS) processes and changes to SMS processes (as defined in the SMS Manual) •Changes to provisions of ATO documents related to separation minima (including waivers) •Controls used by ATO to mitigate hazards with high **initial** safety risk	•Items or changes that require AOV approval •Any change that has high **initial** safety risk •Changes to, or replacement of, a system that if lost or malfunctioning would require application of contingency procedures involving increased separation standards or would result in "ATC Zero" status (e.g., ATOP or C-ARTS) •Changes in the periodicity of maintenance or inspection (including flight inspection) of systems described above (in 3rd bullet)	•Changes with medium or low **initial** safety risk, where safety risk and controls/mitigations: –stay within ATO Service Unit, the SRMD is approved within the Service Unit –span ATO Service Units, the SRMD is approved within each affected Service Unit –go outside of ATO (i.e., to ARP and/or AVR), the SRMD is approved by each affected LOB

* Please note that SRMD approval is not the same as risk acceptance



News and Information
for Air Traffic Organization Employees

www.ato.faa.gov